Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:33:51 UTC

APT group: ToddyCat

Names	ToddyCat *(Kaspersky)* Storm-0247 *(Microsoft)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2020	
Description	(Kaspersky) ToddyCat is a relatively new APT actor that we have not been able to relate to other known actors, responsible for multiple sets of attacks detected since December 2020 against high-profile entities in Europe and Asia. We still have little information about this actor, but we know that its main distinctive signs are two formerly unknown tools that we call ‘Samurai backdoor’ and ‘Ninja Trojan’.	
Observed	Sectors: Defense, Government, Telecommunications. Countries: Afghanistan, India, Indonesia, Iran, Kazakhstan, Kyrgyzstan, Malaysia, Pakistan, Russia, Slovakia, Taiwan, Thailand, UK, Uzbekistan, Vietnam.	
Tools used	China Chopper, Cuthead, FRP, Impacket, Krong, LoFiSe, Ninja, Ngrok, PcExter, PsExec, Samurai, SIMPOBOXSPY, SoftEther VPN, TomBerBil, WAExp.	
Operations performed	2021	Operation “Stayin’ Alive” Unveiling ‘Stayin’ Alive’: A Closer Look at an Ongoing Campaign in Asia Targeting Telecom and Governmental Entities <https://blog.checkpoint.com/security/unveiling-stayin-alive-a-closer-look-at-an-ongoing-campaign-in-asia-targeting-telecom-and-governmental-entities/>
	2024	How ToddyCat tried to hide behind AV software <https://securelist.com/toddycat-apt-exploits-vulnerability-in-eset-software-for-dll-proxying/116086/>
Information	<https://securelist.com/toddycat/106799/> <https://securelist.com/toddycat-keep-calm-and-check-logs/110696/> <https://securelist.com/toddycat-traffic-tunneling-data-extraction-tools/112443/>	

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format
